Planning Guide
Consumerization Security for the Changing Enterprise
Intel’s Guide to Layered Protection

Why You Should Read This Document
This planning guide is designed to help you improve security in today’s changing enterprise environment. With hardware-enhanced security in place, you can gain layered protection for every perimeter of your business, including:

- **Network** – Use powerful authentication technologies to provide network access only to known, trusted users.
- **Platform(s)** – Deploy added protection that works below the operating system to stop attacks in real time and protect online transactions.
- **Applications** – Harden application security to protect operating system vulnerabilities, such as escalation-of-privilege attacks, and better protect virtualized infrastructure models.
- **Data** – Gain greater protection for sensitive business data with faster full-disk encryption and built-in anti-theft capabilities.
- **Remediation** – Respond quickly with remote remediation capabilities, including the ability to diagnose, isolate, and repair infected clients in any operational state, in any location.
Contents

3  Consumerization: Securing a Moving Target
4  More Devices, More Risk
5  Providing Layered Protection: Five Defense Perimeters
9  Intel IT’s Security Strategy: Protect to Enable
11  Move Forward with Confidence
12  Intel Resources for Learning More
Consumerization is reshaping the IT landscape. Cloud and mobility are having a significant long-term impact on global businesses—and there’s no turning back. In the new enterprise environment, IT must secure and manage a multitude of mobile devices and an increasingly diverse set of operating systems to keep workers and the business productive.

Security remains one of the biggest challenges of consumerization, in large part because it’s fueled by constant change: What is the best way to secure data on a growing range of devices in multiple locations? How can I protect network access while ensuring that the right users can get to the right information? In the United States alone, 80 percent of IT managers support consumerization, but security concerns are the top barrier to enabling Bring Your Own Device (BYOD).

Despite complex risks, consumerization offers undeniable productivity benefits. Users with the right business-enabled mobile devices can work more effectively, whenever they can, and from wherever they are. As a result, IT organizations are examining a range of tools, strategies, and technologies to embrace the productivity advantages of both mobility and cloud. The key to success? IT must transform security to protect a moving target.

The Purpose of This Guide

The purpose of this guide is to help you better manage the changing IT security needs of today’s enterprise environment. By adopting a new approach to security architecture that includes hardware-enhanced security technologies, you can gain even greater protection for your business data across a range of devices as you guard against the latest efforts in malware and viruses.

Using the embedded security of Intel® Core™ vPro™ processors and Intel-partner-based software solutions, you can harden protection across five critical security perimeters of your business: your network, platform(s), applications, data, and remediation capabilities. You’ll also gain insight into Intel IT’s approach, which is designed to balance IT security with the flow of information.
More Devices, More Risk

The security landscape is changing fast. The rise of consumerization means more devices; more devices mean greater risk. There is growing support for BYOD initiatives, which have expanded beyond phones and tablets to include personal laptops and even desktop PCs. Many of these consumer devices don’t have the controls to protect sensitive business data, such as corporate IP, customer information, and supplier data. Complicating matters are aging devices that are ill equipped to handle the latest security challenges.

This landscape creates new opportunities for attacks to evade current security models and move down the stack. Cybercriminals are now using stealthy attack methods to hide data-stealing malware, and they’re targeting the enterprise with different goals, from the exfiltration of data and long-term infiltration of corporate networks, to distributed denial-of-service attacks.

Highly targeted malware and viruses are increasing exponentially. Malware is getting more sophisticated, with no sign of slowing down. Consider these facts from 2012:

- New malware samples grew by 50 percent.
- Mobile malware increased by 44 times.
- New ransomware samples soared to over 200,000 per quarter.

A New Approach to Security

Historically, security strategies were designed to protect the network perimeter, but that is no longer enough. Today’s network perimeter has been redefined and expanded by mobile devices, and this makes data protection all the more challenging.

IT must respond with an innovative approach—to protect, but also to predict, detect, and respond swiftly to incidents when they occur. This requires a dynamic, multilayered security approach with technology that not only protects every perimeter of the business, but delivers the right level of system performance and information access to keep users productive and connected.
Providing Layered Protection: Five Defense Perimeters

While software-based solutions are at the foundation of most security management systems, there’s a way to increase that protection below the operating system. By using hardware-enhanced security technologies with the right software, you can strengthen protection for every perimeter of your business.

1. **Network** – Use powerful authentication technologies to provide network access only to known, trusted users.

2. **Platform(s)** – Deploy added protection that works below the operating system to stop attacks in real time and protect online transactions.

3. **Applications** – Harden application security to protect operating system vulnerabilities, such as escalation-of-privilege attacks, and better protect virtualized infrastructure models.

4. **Data** – Gain greater protection for sensitive business data with faster full-disk encryption and built-in anti-theft capabilities.

5. **Remediation** – Respond to events quickly with remote remediation tools, including hardware-based client management and the ability to diagnose, isolate, and repair infected clients in any operational state, regardless of their physical location.

---

**Employ Multiple Security Perimeters**

![Diagram showing multiple security perimeters](image)

- **Network**: Firewalls, demilitarized zone, data loss prevention
- **Platform**: Antivirus software, patching, security specifications for systems
- **Application**: Secure coding, security specifications
- **Data**: File and data encryption, enterprise rights management
- **Response**: Monitoring, intrusion detection, remediation

Figure 2: Security for each layer of the enterprise perimeter.
Perimeter 1: Network

Today’s network perimeter is being redefined by users with mobile devices. Users are accessing information from employer-provided and personally owned devices on both public and private networks around the world. Complicating matters are emerging peer-to-peer device sharing solutions, in which data is transferred directly from machine to machine, bypassing traditional network connections.

While traditional security methods are designed to protect the network with firewalls, access control lists (ACLs), and other methods, they can’t keep all attacks out. Moreover, identity and access management (IDAM) software protections at the traditional network perimeter are no longer sufficient. These factors illustrate how people have become the new business network, making user authentication all the more critical.

By using hardware-enhanced identity management in Intel Core vPro processors, you can help prevent illegitimate users and malware from gaining access to your web sites and virtual private networks (VPNs).

- **Deploy two-factor authentication** – Intel Identity Protection Technology with public key infrastructure (PKI) operates on two levels for stronger two-factor authentication.
  - Prevents screen scraping with built-in protection at the hardware level that hides a user’s keystrokes.
  - Stops illegitimate users from logging in by generating a secure token for each user or client device, which validates that a trusted person (not malware) is logging in from a trusted device.

Perimeter 2: Platform (Device)

If an attack successfully breaks through the network, the platform (or device) is the next stop. To keep viruses and rootkits out, many organizations deploy antivirus and antimalware software. Some use sandboxing to isolate applications, in which programs and processes can run in an isolated virtual environment. However, attacks can still get through, sometimes using weak security keys, rootkits, drive-by downloads, and other methods.

To protect critical data at the platform level, hardware and software must work together at different security points. By using Intel Core vPro processors with McAfee software, you can protect your platform with technologies that work below the operating system to stop attacks in real time.

- **Detect new stealth attacks as they happen** – McAfee Deep Defender hardware-enhanced security uses McAfee DeepSAFE technology with Intel Virtualization Technology to monitor kernel memory in real time, even before the operating system boot loader starts. With Intel Core vPro processors, this unique solution works beyond the operating system for zero-day protection—the ability to detect, block, quarantine, and remove stealthy threats before harm is done—without requiring any prior knowledge of the threat.

- **Protect online transactions** – Built into Intel Core vPro processors is Intel Secure Key, which generates higher-quality random numbers so that data encryption is even more secure. Because this encryption technology is hardware based, it is extremely resistant to hacking. This technology delivers:
  - High-quality random numbers from a high-volume entropy source, making the numbers unpredictable
  - High performance that is faster than most entropy sources available today
  - Easy access, with instruction available to all applications and at any privilege level
  - Secure hardware-based implementation that isolates the entropy source from software attack
Perimeter 3: Application

After reaching the platform, the next step for hackers is the application perimeter. Hackers often attack by trying to gain certain privileges or by promoting attacks inside unsecured applications. In addition, there is an increasing reliance on virtualization to enable more flexible client computing solutions, such as sharing work and personal information on a single device. As companies adopt shared, multitenant, virtualized infrastructure models, they are exposing vulnerabilities across a wider range of applications.

By using hardware-enhanced application isolation containers, you can better protect operating system vulnerabilities such as escalation-of-privilege attacks. Because Intel vPro technology is embedded at the hardware level, it can protect against evasive, penetrating rootkits and malware that threaten users working in traditional operating system, cloud, or virtual application environments. The technology capabilities are accessed and administered separately from the hard drive, operating system, and software applications in a preboot environment.

• **Work confidently with a secure boot process** – Intel Trusted Execution Technology7 (Intel TXT) works with Intel Virtualization Technology to protect your IT infrastructure against software-based attacks by validating the behavior of key components within the PC at start-up. Using a “root-of-trust” infrastructure, Intel TXT provides an additional enforcement point using a verification process based on a “known good” sequence, which checks for malicious software on client and server platforms before launch.

• **Keep attacks from taking hold** – Prevent attacks from digging in below the operating system where they can do the most damage. Intel Platform Protection Technology with Boot guard8 delivers built-in protection against multiple methods of escalation-of-privilege attacks, which occur when a hacker gains elevated access to your network and its associated data and applications.

• **Gain further protections against viruses** – Traditional security approaches are only partially effective at managing the increasing volume and sophistication level of today's attacks. By using McAfee VirusScan* software in desktop mode on Windows* 8, you can gain added protection for the full range of threat targets—popular browsers, plug-ins, networks, databases, mobile devices, web, e-mail, and more.

Perimeter 4: Data

Most attacks are ultimately trying to reach the data layer, where your intellectual property and corporate value sit. Data loss from unsecured mobile devices is one of the biggest risks to enterprises today. In fact, a study by Solera Networks and the Ponemon Institute revealed that “on average, malicious—or intentional—breaches cost affected organizations $840,000 in overall impact, compared with $470,000 for non-malicious data loss incidents.” The research also revealed that the average malicious data breach took 80 days to detect, and more than four months to resolve.

While nearly all IT organizations have data protection and encryption security in place, encryption technologies can have a significant impact on system performance and user productivity. It's enough to cause some organizations to wonder if the benefits outweigh the hassles.

With the hardware-based data protection of Intel vPro technology, you can gain even greater protection for sensitive business data. Because it runs in the background and doesn't drain resources, it won't interrupt users while they're working.

• **Work with faster encryption** – Intel Advanced Encryption Standard New Instructions9 (Intel AES-NI) delivers accelerated hardware-based encryption up to four times faster,10 and it works quietly in the background without slowing performance or interfering with user productivity. In addition, Intel AES-NI forms the secure backbone of McAfee Endpoint Encryption technologies by helping users maintain productivity while protecting data on PCs.

• **Gain at-rest data protection** – The Intel Solid-State Drive (SSD) Pro family11 disk storage provides on-board, accelerated full-disk encryption capabilities.

• **Get built-in anti-theft capabilities** – If a device is lost or stolen, Intel Anti-Theft Technology12 (Intel AT) works to protect your data under any circumstances. The technology can automatically disable the device locally if it's been hacked, or remotely, after it's been reported as lost or stolen. If the device is recovered, IT can remotely reactivate the device without any data loss.
Perimeter 5: Remediation

Considering the advanced nature of today’s cybercrime attacks, some are bound to get through even the most sophisticated security infrastructures. Moreover, a distributed mobile workforce can complicate remediation efforts, especially when IT team members are probably not in the same location as the compromised device. Since no degree of protection is 100 percent guaranteed, IT must put in place a proactive approach to remediation that includes:

- Detecting and containing the threat
- Minimizing or eliminating data loss
- Implementing a plan of resilience for recovery
- Correcting the problem quickly

One critical aspect of remediation is reducing the time it takes to detect, stop, contain, and recover data while getting enterprise users back up and running. You can do this by implementing robust remediation capabilities that give you the ability to respond from any location, at any time:

- **Work with powerful remote management** – You can use Intel Active Management Technology (Intel AMT) to remotely diagnose, isolate, and repair infected clients—regardless of their operational state.

- **Strengthen endpoint security** – McAfee ePolicy Orchestrator (McAfee ePO) Deep Command uses Intel vPro technology to take security management beyond the operating system to manage security at the hardware level. With McAfee ePO Deep Command, IT administrators can control powered-off or disabled endpoints to run security updates, deployment, and remediation tasks.

An Alternative to Mobile Device Management

Mobile devices such as smart phones and tablets are rapidly becoming the next-generation endpoint clients for businesses. While mobile device management (MDM) software is a common method of managing these devices, there is another way. With any Intel® architecture-based device running Windows® 8 Pro or Windows 8 Enterprise, you have an end-to-end device management solution for tablets, notebooks, and desktops through Microsoft® System Center Configuration Manager (SCCM) 2012.

Windows 8 technology is compatible with traditional Windows desktop applications, peripherals, and drivers that span most enterprise environments, so it’s a natural fit. It works easily with legacy systems and delivers innovative touch capabilities to those workers who need it, without any additional software or hardware. Moreover, these devices are available in a range of form factor options, with power that ranges from Intel Atom™ processors to Intel Core™ vPro™ processors.
Intel is facing the same challenges around consumerization as any enterprise, including finding that elusive balance between IT security and the flow of information. Intel’s new information security strategy, “Protect to Enable,” is designed to enable information flow, which increases productivity and agility while decreasing risk.

At the foundation of Protect to Enable is a dynamic trust model that adjusts based on several factors: the employee’s authentication method; the application they want to use; the data they want to access; the “trust level” of their device; and their location, whether at a work site (connecting via a secure corporate network) or off-site (connecting via a public network). Intel IT also uses this trust model as the basis for deciding when and how sensitive data and services can be moved into the cloud.

**Protect to Enable: The Four Cornerstones**

Intel IT’s innovative Protect to Enable strategy is based on the following four cornerstones:

1. **Trust calculation** – Determines who wants what information where, and from what device, with permission levels that adjust based on the security of the location for the user and device

2. **Balanced controls** – Investing in solutions that balance attack prevention with detection and correction solutions, enabling organizations to react to and quickly recover from inevitable attacks

3. **User and data perimeters** – Expands perimeters to include both users and data instead of just the network

4. **Security zones** – High-security zones for critical data, and less secure zones for other data

Figure 3. Protect to Enable at a glance. Source: Intel IT.
Another key component of the Protect to Enable strategy is Intel IT’s Security Business Intelligence (SBI) platform. The primary goals of the SBI platform are to:

- Build a cost-effective solution that maintains regulatory compliance, keeps information available, and protects data.
- Use advanced analytics (such as big data) to improve the ability to predict, detect, prevent, and respond to cyber threats and incidents.
- Use the results to identify less effective security controls to either improve or eliminate them.

Recognizing that protecting employee privacy is paramount, the Intel IT SBI platform was designed with Intel’s established privacy principles from the beginning. This privacy implementation included the following steps:

1. Educate key stakeholders on privacy principles before design and deployment to ensure that all parties understand, respect, and abide by Intel’s privacy policies.
2. Define and implement policies and processes to ensure appropriate management of personal information throughout the data life cycle.

The SBI platform incorporates a large-scale common logging service (CLS) and various custom analytics platforms. The ability to implement custom analytics solutions quickly enables the Intel security team to filter and distill specific event logs from over 6 billion events recorded daily. Benefits include improved compliance, better protection of high-risk assets, and a faster, more intelligent response to advanced persistent threats (APTs).

Intel IT is continuing to scale the SBI platform to increase its ability to proactively find advanced threats, react quickly, and develop preventive and corrective controls for the future. We are also looking at ways to leverage trusted sensor and event information to improve platform quality and reliability.

Intel IT Furthers Protection with McAfee* Deep Defender*

Intel IT continues to evolve and improve its security protection with advanced capabilities. The organization recently piloted McAfee Deep Defender to help protect against malware threats. During the pilot, McAfee Deep Defender detected and blocked malware that no application currently deployed at Intel could have prevented in such a timely manner. Based on these results, Intel is conducting a production pilot targeting internal organizations and will assess wider deployment in the second half of 2013.

Security Business Intelligence Platform Capabilities

The Security Business Intelligence platform at Intel IT.

Security Business Intelligence

Dashboards, Risk Reporting, and Automated Incident Response

Proxy, DNS, DHCP, Active Directory*, Management Platforms, Contextual

Extraction and Load

Data Storage and Analysis

Reporting and Workflow Automation

Common Logging Service

Extreme Data Warehouse

Real-Time Correlation

Security Sensors

Figure 4. The Security Business Intelligence platform at Intel IT.
Move Forward with Confidence

The IT security landscape will continue to change and grow with new devices and technologies, increased cloud implementations, and expanded mobile capabilities. Security challenges will persist, and advanced threats will continue to evolve at an equally fast pace. By implementing a new security approach with layered protection, IT can gain the increased security it needs while users get the flexibility they need to stay productive from any location, on any device. This requires advanced protection for all five layers of the enterprise: network, platform(s), applications, data, and remediation.

Intel is continuing to develop innovative ways to increase security for the enterprise environment while making it easier for users to work quickly and efficiently. This includes the ability to prevent, detect, and respond to cyber threats—an inevitable component of today’s security landscape.

Within Intel, Intel IT has taken proactive steps to embrace consumerization by re-engineering its security architecture to better protect the business. The organization is constantly evolving its security capabilities by deploying advanced protection. And after a successful testing phase, the trust model is in place to help further reduce enterprise risk with dynamic security controls, while improving the user experience across a range of devices.

Hardware-enhanced security from Intel and its ecosystem partners is designed to harden protection at all perimeters of your enterprise—for tablets, notebooks, phones, and desktop PCs. Intel vPro technology is a growing suite of security, management, and business productivity technologies that are designed to meet IT security needs while delivering built-in protection for business data. And the latest 4th generation Intel Core vPro processor comes with new enhancements that can improve productivity for your users and increase security for your business devices. Today and into the future, Intel will continue its ongoing commitment of delivering innovative, secure business technologies so that your organization can move forward with confidence.

Security Enhancements in Intel® vPro™ Processors

The latest enhancements in the 4th generation Intel® Core™ vPro™ processor will be introduced across a range of business-class devices, including Ultrabook™ devices, tablets, notebooks, and desktop PCs.

- Protect data around the clock with automatic encryption from the integrated Intel Solid-State Drive Pro family and remote anti-theft capabilities.
- Simplify password management with a “no password” VPN experience that safeguards your network and helps users stay focused on the task at hand.
- Manage devices with greater control, regardless of whether they are connected to the network, powered off, lost, or stolen.
- Remotely track and manage thousands of devices with update, disable, lock, wipe, or restore capabilities.
- Help improve your desktop virtualization experience with enhanced PC performance and graphics using Intel Virtual Machine Control Structure Shadowing (Intel VMCS).
Intel Resources for Learning More

**General Information**

For general information about consumerization, visit [intel.com/consumerization](http://intel.com/consumerization).

Or visit the following web sites:

- Intel vPro technology: [intel.com/vpro](http://intel.com/vpro)
- McAfee Deep Defender: [mcafee.com/deepdefender](http://mcafee.com/deepdefender)
- McAfee DeepSAFE technology: [mcafee.com/deepsafe](http://mcafee.com/deepsafe)
- McAfee ePO Deep Command: [mcafee.com/deepcommand](http://mcafee.com/deepcommand)

**Additional Resources**

**Five Steps to Consumerization of IT in the Enterprise**

This planning guide outlines five steps to help you manage consumerization with a user-centered strategy that supports employee-owned and employer-provided devices side-by-side.


**Future Implications of Consumerization in the Enterprise**

Discover Intel's vision of the future of IT in a consumerized world, in which IT empowers mobile users to create, consume, and share data using any device, in any environment.


**Inside IT: Balancing Security and a Great User Experience**

Listen to Toby Kohlenberg, Intel IT senior information security technologist, discuss Intel's new trust model and the challenges of balancing security with a great user experience.


**Intel IT's New Information Security Strategy**

Watch this video and find out how Intel IT is tackling consumerization with a new information security strategy that increases productivity and innovation while actually decreasing risk.


2. Intel vPro technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit [intel.com/technology/vpro](http://intel.com/technology/vpro).


4. No system can provide absolute security under all conditions. Requires an Intel Identity Protection Technology–enabled system, including a 2nd gen or higher Intel Core processor-enabled chipset, firmware and software, and a participating web site. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems, or any resulting damages. For more information, visit [http://ipt.intel.com](http://ipt.intel.com).

5. Intel Virtualization Technology requires a computer system with an enabled Intel processor and BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit [intel.com/content/www/us/en/virtualization/virtualization-technology/hardware-assist-virtualization-technology.html](http://intel.com/content/www/us/en/virtualization/virtualization-technology/hardware-assist-virtualization-technology.html).

6. No system can provide absolute security. Requires an Intel Secure Key–enabled PC with an Intel Core vPro processor and software optimized to support Intel Secure Key. Consult your system manufacturer for more information.

7, 8, 12. No computer system can provide absolute security. Requires an enabled Intel processor, enabled chipset, firmware, and software, and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your service provider for availability and functionality. For more information, visit [intel.com/go/anti-theft](http://intel.com/go/anti-theft) or consult your system manufacturer and/or software vendor.

9. No computer system can provide absolute security. Requires an enabled Intel processor and software optimized for use of the technology. Consult your system manufacturer and/or software vendor for more information.

10. Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests such as SYSmark* and MobileMark* are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

11. No computer system can provide absolute security under all conditions. Built-in security features available on select Intel Solid-State Drives may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details.

13. Requires activation and a system with a corporate network connection, an Intel AMT–enabled chipset, and network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a VPN based on a host operating system or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit [intel.com/content/www/us/en/architectures-and-technology/intel-active-management-technology.html](http://intel.com/content/www/us/en/architectures-and-technology/intel-active-management-technology.html).
More from the Intel® IT Center

This planning guide, Consumerization Security for the Changing Enterprise, is brought to you by the Intel® IT Center, Intel’s program for IT professionals. The Intel IT Center is designed to provide straightforward, fluff-free information to help IT pros implement strategic projects on their agenda, including virtualization, data center design, intelligent clients, and cloud security. Visit the Intel IT Center for:

- Planning guides, peer research, and solution spotlights to help you implement key projects
- Real-world case studies that show how your peers have tackled the same challenges you face
- Information on how Intel’s own IT organization is implementing cloud, virtualization, security, and other strategic initiatives
- Information on events where you can hear from Intel product experts as well as from Intel’s own IT professionals

Learn more at intel.com/ITCenter.